Certificate of Cloud Auditing Knowledge (CCAK) Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The rapidly accelerating pace of Digital Transformation mandates that IT audit professionals evolve their skills from traditional, perimeter-based security reviews to modern, platform-agnostic evaluation methodologies. Certificate of Cloud Auditing Knowledge (CCAK) Training Course is the premier credential, co-developed by the Cloud Security Alliance and ISACA, designed to bridge the technical knowledge gap between cloud security concepts and robust Cloud Governance frameworks. Professionals will master the complexities of the Shared Responsibility Model, learning to accurately define and audit customer controls versus provider controls (CSP) across IaaS, PaaS, and SaaS, ensuring comprehensive Risk Mitigation and maintaining Continuous Assurance in dynamic, Hybrid Cloud environments.

This course moves beyond foundational concepts to focus on high-priority, trending audit challenges, including the implementation of Zero Trust Architecture, the security posture of Cloud-Native workloads, and compliance with global Data Sovereignty and privacy laws. We emphasize the practical application of essential industry tools, notably the Cloud Controls Matrix and the Consensus Assessments Initiative Questionnaire. Graduates will be equipped to evaluate automated compliance through DevSecOps pipelines and leverage Generative AI and Real-Time Auditing tools to enhance audit efficiency and uphold organizational reputation in the era of pervasive, multi-cloud computing.

Programme Curriculum

Certificate of Cloud Auditing Knowledge (CCAK) Training Course

Introduction

The rapidly accelerating pace of Digital Transformation mandates that IT audit professionals evolve their skills from traditional, perimeter-based security reviews to modern, platform-agnostic evaluation methodologies. Certificate of Cloud Auditing Knowledge (CCAK) Training Course is the premier credential, co-developed by the

Cloud Security Alliance and ISACA, designed to bridge the technical knowledge gap between cloud security concepts and robust Cloud Governance frameworks. Professionals will master the complexities of the Shared Responsibility Model, learning to accurately define and audit customer controls versus provider controls (CSP) across IaaS, PaaS, and SaaS, ensuring comprehensive Risk Mitigation and maintaining Continuous Assurance in dynamic, Hybrid Cloud environments.

This course moves beyond foundational concepts to focus on high-priority, trending audit challenges, including the implementation of Zero Trust Architecture, the security posture of Cloud-Native workloads, and compliance with global Data Sovereignty and privacy laws. We emphasize the practical application of essential industry tools, notably the Cloud Controls Matrix and the Consensus Assessments Initiative Questionnaire. Graduates will be equipped to evaluate automated compliance through DevSecOps pipelines and leverage Generative AI and Real-Time Auditing tools to enhance audit efficiency and uphold organizational reputation in the era of pervasive, multi-cloud computing.

Course Duration

10 days

Course Objectives

1. Master the application of the CSA CCM v4 and CAIQ for effective cloud security assessment and vendor selection.
2. Design and evaluate holistic, platform-agnostic Cloud Governance programs aligned with organizational strategy and business objectives.
3. Implement and audit Zero Trust Architecture principles, focusing on microsegmentation and continuous verification.
4. Conduct comprehensive Threat Modeling and risk analysis specific to FaaS and Container workloads.
5. Evaluate compliance with complex global Data Sovereignty and data residency requirements
6. Audit the security and compliance controls embedded within DevSecOps and continuous integration/continuous delivery (CI/CD) pipelines.
7. Develop strategies for achieving Continuous Monitoring and real-time assurance using native CSP tools and RegTech solutions.
8. Assess the effectiveness of Confidential Computing and advanced cryptographic controls for data processing in the cloud.
9. Audit financial efficiency and policy enforcement within a FinOps framework to ensure cost-aware control implementation.
10. Analyze and evaluate Service Level Agreements and contracts in the context of the Shared Responsibility Model to mitigate third-party risk.
11. Implement proper Cloud Forensics procedures and audit logs necessary for incident response and legal hold scenarios.
12. Integrate the governance and audit requirements for using Generative AI models and platforms securely.
13. Prepare for the CCAK examination with confidence, demonstrating expertise in Cloud Audit Characteristics and principles.

Target Audience

1. IT Auditors
2. Information Security Officers
3. Cloud Security Professionals and Architects
4. Compliance and Risk Managers

5. Data Protection Officers
6. Third-Party Risk Assessors
7. Security and Privacy Consultants
8. IT Governance and Assurance Professionals

Course Modules

Module 1: Cloud Governance and Organizational Strategy

- Overview of Cloud Risk Management and its integration into Enterprise Risk Management
- Establishing cloud governance structures, roles, and responsibilities
- Defining and auditing the cloud operating model and policy-as-code deployment.
- Evaluating the impact of cloud strategy on organizational culture and skill gaps.
- Implementing metrics and Key Risk Indicators for cloud environments.
- Case Study: Auditing a global financial institution's transition from traditional IT audit to a Cloud Center of Excellence governance model, focusing on initial risk acceptance criteria and policy definition across multi-region deployments.

Module 2: Legal, Regulatory, and Data Sovereignty

- Understanding and mapping compliance requirements to cloud controls.
- Auditing Data Residency and jurisdictional compliance for global data deployments.
- Reviewing the legal and contractual implications of using foreign Cloud Service Providers
- The auditor's role in assessing privacy impact assessments and data mapping.
- Navigating the regulatory differences between IaaS, PaaS, and SaaS environments.
- Case Study: A healthcare provider expanding internationally faces a GDPR violation risk. Audit the organization's data classification and regional access controls to ensure ePHI remains within required sovereign borders.

Module 3: Auditing the Shared Responsibility Model

- Detailed breakdown of the Shared Responsibility Model across all cloud deployment and service models.
- Analyzing Service Organization Control reports and other third-party attestations from CSPs.
- Techniques for scoping audit efforts to focus strictly on the Customer's Shared Responsibility controls.
- Reviewing Cloud Service Agreements and SLAs for appropriate liability and security guarantees.
- Verifying the CSP's adherence to security baselines using the CSA STAR registry.
- Case Study: An e-commerce company migrating to PaaS relies heavily on the CSP for runtime security. Audit the contract and the company's internal process for reviewing the CSP's SOC 2 report, identifying key control gaps in their application code and configuration management.

Module 4: CSA Cloud Controls Matrix Deep Dive

- In-depth structure and purpose of the CCM v4 and its alignment with major security standards
- Utilizing CCM control IDs for consistent, cross-functional communication and reporting.
- Applying the CCM to different cloud delivery models for control mapping.
- Customizing the CCM for specific organizational risk profiles and compliance scopes.
- Auditing evidence collection strategies tailored to CCM control requirements.
- Case Study: Use the CCM to map control requirements for a PaaS deployment, creating a bespoke audit checklist that validates controls in the Application Security and Configuration Management domains.

Module 5: Consensus Assessments Initiative Questionnaire (CAIQ)

- Purpose and methodology of the CAIQ for cloud provider assessment and due diligence.
- Analyzing vendor responses to the CAIQ to identify security and compliance gaps.
- Integrating CAIQ results into the organization's Third-Party Risk Management program.
- Using the CAIQ as a basis for customized procurement and contract negotiation questions.
- Leveraging CAIQ data for internal gap analysis against corporate security policies.
- Case Study: An organization is evaluating two competing SaaS providers. Use their publicly available CAIQ responses to compare their security postures in the Identity and Access Management and Encryption & Key Management domains, recommending the lower-risk vendor.

Module 6: Cloud Threat and Risk Analysis Methodology

- Introduction to cloud-specific threat modeling techniques
- Analyzing common cloud security risks.
- Conducting risk assessments based on the likelihood and impact of common cloud vulnerabilities.
- Using the CCM's Threat Analysis section to prioritize audit focus areas.
- Developing risk treatment plans based on audit findings.
- Case Study: Perform a Threat Analysis on a public-facing IaaS deployment hosting a legacy application. Identify the risks associated with an exposed database, focusing on the likelihood of a SQL Injection attack and recommending compensating controls.

Module 7: Audit Planning for Multi-Cloud Environments

- Strategies for unifying audit efforts across diverse public cloud platforms.
- Techniques for creating an effective cloud audit program scope, including selection of audit targets
- Planning for evidence collection and sampling in highly ephemeral and scalable environments.
- Establishing audit criteria using internal policies, regulatory requirements, and industry standards
- Developing communication strategies for engaging with both cloud engineering and business teams during the audit.
- Case Study: A multinational company uses a Multi-Cloud strategy. Plan a 6-week audit to cover core services across two different CSPs, ensuring consistent application of the organization's Data Protection policy in both environments.

Module 8: Auditing Identity and Access Management (IAM)

- Auditing the implementation of the Principle of Least Privilege across all cloud accounts.
- Reviewing configuration of cloud-native IAM services for policy gaps.
- Assessing the maturity and enforcement of Zero Trust Architecture components like conditional access and micro-segmentation.
- Testing for the mandatory use and configuration of Multi-Factor Authentication for privileged users.
- Auditing federated identity and access management integration points.
- Case Study: Audit a security breach involving Compromised Credentials. Analyze access logs and IAM policies to determine where the Least Privilege principle failed and recommend stronger access controls.

Module 9: Auditing DevSecOps and CI/CD Pipelines

- Integrating audit checkpoints into the DevSecOps lifecycle
- Auditing security tools and practices within the CI/CD pipeline
- Reviewing the security of Infrastructure-as-Code (IaC) templates for misconfigurations.
- Assessing the change control and approval processes within automated deployment pipelines.
- Evaluating the use of secure secrets management vaults in the development workflow.

- Case Study: Audit a development team's CI/CD pipeline for non-compliance. Review their automated security scanning results, focusing on identifying hardcoded secrets and unvalidated open-source dependencies before deployment.

Module 10: Auditing Containerization and Serverless Functions

- Auditing container image hygiene, hardening practices, and vulnerability scanning in registries
- Reviewing the security configuration of orchestrators like Kubernetes
- Assessing the unique security posture and configuration of Serverless functions and APIs.
- Testing runtime security and configuration drift detection for cloud-native workloads.
- Evaluating network segmentation controls within containerized environments.
- Case Study: A company running microservices on Kubernetes needs an audit. Focus on the Pod Security Policies and Role-Based Access Control to ensure containerized applications cannot perform privileged actions.

Module 11: Continuous Compliance and Monitoring

- Establishing a framework for Continuous Compliance and real-time control validation.
- Using Cloud Security Posture Management tools for automated configuration auditing.
- Implementing Regulatory Technology solutions for automated evidence collection and reporting.
- Auditing the effectiveness of alert management, SIEM integration, and log retention policies.
- Developing customized dashboards and metrics for reporting Continuous Assurance status to the board.
- Case Study: Implement and audit a CSPM solution within a highly dynamic environment, verifying that automated remediation workflows are not introducing new operational risks while correcting policy violations.

Module 12: Cloud Forensics and Incident Response Audit

- Auditing the organization's Cloud Incident Response plan for cloud-specific scenarios
- Reviewing log and audit trail capabilities for forensic readiness, including retention and immutability.
- Assessing the technical procedures for collecting and preserving volatile evidence in cloud environments.
- Evaluating the use of cloud-native tools for security information and event management and security orchestration, automation, and response.
- Auditing procedures for secure termination and de-provisioning of cloud assets post-incident.
- Case Study: A company experiences a suspected Cloud Account Compromise. Audit the incident response team's log analysis capabilities, focusing on the ability to trace the attacker's actions and ensure chain of custody for digital evidence.

Module 13: Data Protection and Confidential Computing Audit

- Auditing data classification, encryption at rest and in transit, and key management service policies.
- Reviewing the security configuration of cloud storage services for public exposure risks.
- Assessing the implementation of Confidential Computing for sensitive processing workloads.
- Auditing Data Loss Prevention tools and policies for effectiveness across multi-cloud endpoints.
- Evaluating the use of data masking, tokenization, and anonymization techniques for compliance.
- Case Study: A financial company is storing highly sensitive transaction data. Audit their Key Management Service configuration, ensuring customer-managed keys are used, rotation policies are enforced, and access logs are tightly controlled and monitored.

Module 14: Auditing FinOps and Resource Optimization

- Understanding the intersection of FinOps principles with security and compliance.
- Auditing the organization's resource tagging and inventory management practices for accountability.
- Reviewing policies governing the secure deletion and de-provisioning of unused cloud resources to reduce both cost and attack surface.
- Evaluating automated resource lifecycle management tools from an audit and compliance perspective.
- Assessing the impact of security control choices on cloud costs and resource efficiency.
- Case Study: Audit a team that left resources running over a holiday weekend, resulting in $50,000 in unnecessary compute charges. Review the automated shutdown policies and the approval process for resource exceptions, recommending controls to enforce cost governance.

Module 15: CSA STAR Program and Vendor Assurance

- Overview of the CSA STAR Program and its three levels.
- Auditing a CSP's self-assessment documentation and public-facing registry submission.
- Understanding and evaluating the requirements for a STAR Level 2 certification/attestation
- Developing internal procedures for continuous monitoring of third-party cloud vendors.
- Synthesizing findings from CCM, CAIQ, and STAR documentation for a holistic vendor risk score.
- Case Study: A company selects a new HR SaaS provider that claims STAR Level 2 certification. Audit their public STAR registry entry, comparing their claimed controls against the organization's own baseline requirements before finalizing the contract

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
23 Nov 2026	04 Dec 2026	Online	$2,000
23 Nov 2026	04 Dec 2026	Physical	$3,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$6,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$9,000
23 Nov 2026	04 Dec 2026	Physical	$12,000
23 Nov 2026	04 Dec 2026	Physical	$12,000

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com